Report No. DODIG-2015-180

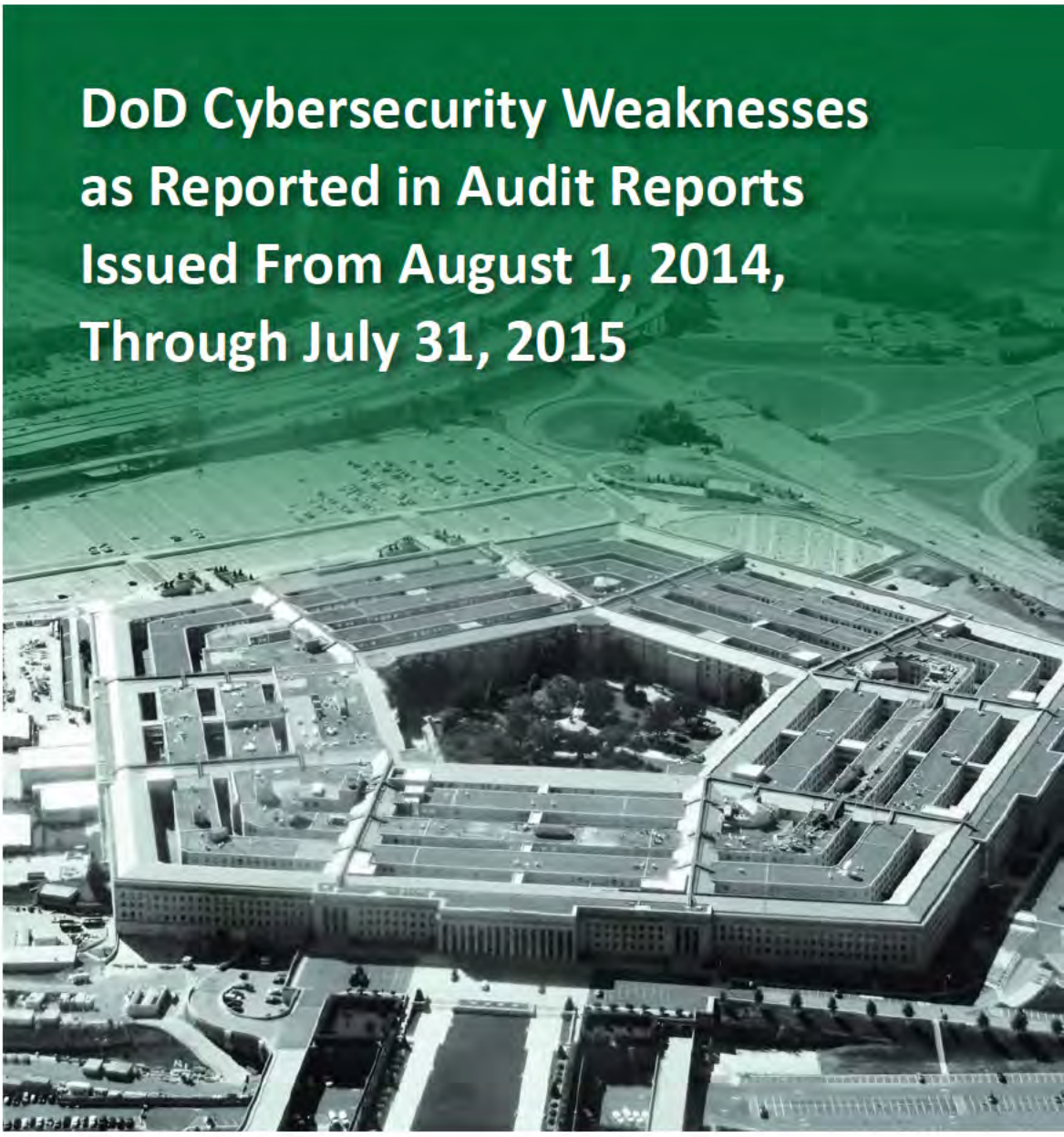
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

SEPTEMBER 25, 2015

DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~FOR OFFICIAL USE ONLY~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015

September 25, 2015

Objective

We summarized DoD and Government Accountability Office audit reports and testimonies issued from August 1, 2014, through July 31, 2015, that contained findings on DoD cybersecurity weaknesses. This summary report supports the DoD Office of Inspector General's (DoD OIG) response to the requirements of Public Law 107-347, Title III, "Federal Information Security Management Act (FISMA)," section 3545, December 17, 2002.

This report is the 17th cybersecurity summary report issued by the DoD OIG since January 1999. This year's cybersecurity weakness categories are consistent with the Department of Homeland Security FY 2015 FISMA Inspectors General reporting metrics.

Results

During the reporting period, the DoD audit community and Government Accountability Office issued 20 unclassified reports and one testimony that addressed a wide range of cybersecurity weaknesses within DoD systems and networks. Reports issued during the reporting period most frequently cited cybersecurity weaknesses in the categories of risk management, identity and access management, and contingency planning.

Visit us on the web at www.dodig.mil

Results (cont'd)

As of August 1, 2014, unclassified audit reports identified in the previously issued cybersecurity summary reports contained 229 unresolved cybersecurity-related recommendations. From August 1, 2014, through July 31, 2015, DoD management resolved 93 recommendations, leaving 136 unresolved cybersecurity-related recommendations that required management action.

Recommendations

In this summary report, we identified recommendations from previously issued reports. Therefore, this report contains no new recommendations and is provided for information purposes only.

Management Comments

We did not issue a draft report because this report consolidates audit findings from audit reports issued from August 1, 2014, through July 31, 2015. No written response is required.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

September 25, 2015

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
MANAGING DIRECTOR, INFORMATION TECHNOLOGY,
GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015 (Report No. DODIG-2015-180)

We are providing this summary report for your information and use. Civil service and uniformed officers who develop, operate, or manage DoD information systems should read this report to be aware of identified cybersecurity challenges in the DoD information technology environment. The overall objective was to summarize the DoD cybersecurity weaknesses identified in unclassified audit reports and testimonies issued by the DoD audit community and the Government Accountability Office from August 1, 2014, through July 31, 2015. During the reporting period, the DoD audit community and the Government Accountability Office issued 20 unclassified reports and one testimony addressing cybersecurity weaknesses within DoD systems and networks.

The report contains no recommendations for action; however, it does identify previously issued audit reports that contain open recommendations. We did not issue a draft report, and no written response is required.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699[(b) (6)] (DSN 499[(b) (6)].

[(b) (6)]
for Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Objective

Our objective was to summarize DoD cybersecurity weaknesses identified in audit reports and testimonies issued by the DoD audit community and the Government Accountability Office (GAO) from August 1, 2014, through July 31, 2015. See Appendix A for a discussion on the scope and methodology and prior coverage related to the objective.

Background

This report is the 17th annual cybersecurity summary the DoD Office of Inspector General (DoD OIG) has issued since January 1999. This report is a reference for identifying audit reports and testimonies that outline DoD cybersecurity weaknesses as related to Public Law 107-347, Section 3545, Title III, "Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

FISMA Requires Security Controls Over Federal Information

Federal Government agencies have a responsibility to protect their information and information systems. This responsibility is promulgated in FISMA, which provides a comprehensive framework for ensuring the effectiveness of agency information security controls. FISMA requires that each agency develop, document, and implement an agency-wide information security program to protect the information and information systems that support agency operations and assets. Each agency must comply with FISMA and related policies, procedures, standards, and guidelines, including the information security standards issued under section 11331, title 40, United States Code, "Responsibilities for Federal Information Systems Standards." FISMA requires that each agency with an Inspector General appointed under the Inspector General Act of 1978, as amended, independently evaluate the effectiveness of their respective agency's information security program and practices. Due to the size and number of DoD organizations, a conclusive annual evaluation of DoD's information security program for each of the FISMA metrics is not practical. Instead, the DoD OIG uses this summary of unclassified cybersecurity-related audit reports and testimonies issued by the DoD audit community and GAO during the reporting period to support the DoD OIG's annual FISMA requirement.

Cybersecurity Weakness Categories

In 2010, the Office of Management and Budget mandated that the Department of Homeland Security provide guidance and operational oversight for Federal agency FISMA reporting. In accordance with that mandate, the Department of Homeland Security develops and issues annual FISMA reporting metrics for Federal agency Inspectors General, Chief Information Officers, and the Senior Agency Officials for Privacy. The Inspector General, Chief Information Officer, and Senior Agency Official for Privacy assess their agency information security controls based on their set of metrics and compile the results in a single FISMA assessment report to the Office of Management and Budget. The annual reports are submitted electronically in CyberScope, an automated platform for secure FISMA reporting.

On December 18, 2014, the Department of Homeland Security issued "FY 2015 Inspector General Federal Information Security Management Act Reporting Metrics, v1.1[1]," which contains the Inspector General reporting metrics. The FY 2015 reporting metrics are:

- Configuration Management,
- Contingency Planning,
- Continuous Monitoring Management,
- Contractor Systems,
- Identity and Access Management,
- Incident Response and Reporting,
- Plan of Action & Milestones,
- Remote Access Management,
- Risk Management, and
- Security Training.

To provide an efficient and effective DoD OIG response to the FISMA requirements, the DoD OIG categorizes the cybersecurity-related audit report and testimony findings by cybersecurity weakness categories, consistent with the 10 Department of Homeland Security FY 2015 FISMA Inspectors General reporting metrics. See the Glossary for definitions of each cybersecurity weakness category.

[1] Department of Homeland Security updated the FISMA reporting metrics "FY 2015 Inspector General Federal Information Security Modernization Act Reporting Metrics V1.2," dated June 19, 2015, to add the Information Security Continuous Monitoring Maturity Model. The reporting metrics remained the same as previous version.

DoD Cybersecurity Instructions and Directives

DoD has issued cybersecurity guidance consistent with the FISMA reporting metrics, which are listed below.

- DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, establishes a DoD cybersecurity program to protect and defend DoD information and information technology (IT).
- DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, establishes policy and assigns responsibility for executing and maintaining the DoD IT risk management framework. This policy provides guidance for the transition from DoD Information Assurance Certification and Accreditation Process (DIACAP) to the RMF.
- DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, establishes policy for securing unclassified information on non-DoD information systems.
- DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014, establishes policy for the respect and protection of an individual's personal information and fundamental right to privacy.
- DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009, establishes that DoD investments in information solutions be managed through a capital planning process that (1) is performance- and results-based, (2) provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks, (3) interfaces with DoD key decision support systems, and (4) requires the review of IT investments for compliance with architectures, IT standards, and related policy requirements.
- DoD Directive 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, certified current as of April 23, 2007, establishes policy and assigns responsibility for DoD information assurance training, certification, and workforce management.

Results

DoD Audit Community and GAO Identified DoD Cybersecurity Weaknesses

From August 1, 2014, through July 31, 2015, the DoD audit community and GAO issued 20 unclassified reports and one testimony that identified a wide range of cybersecurity weaknesses within DoD systems and networks. The reports and testimony identified issues in 9 of the 10 FISMA reporting metrics. The DoD audit community and GAO provided 49 recommendations related to the FY 2015 FISMA reporting metrics to correct cybersecurity weaknesses.

Cybersecurity Weaknesses Identified in Audits and Testimony

This report summarizes the cybersecurity weaknesses identified in DoD audit community and GAO reports and testimony as they relate to the FY 2015 FISMA reporting metrics. Table 1 shows the number of cybersecurity weaknesses identified in the 20 reports and one testimony, related to the FY 2015 FISMA reporting metrics.

Table 1. Cybersecurity Weaknesses Reported From August 1, 2014, Through July 31, 2015

FISMA Reporting Metrics	GAO	DoD OIG	Military Departments	Total
Risk Management	2	2	13	17
Identity and Access Management	0	1	10	11
Contingency Planning	1	0	7	8
Configuration Management	0	2	5	7
Continuous Monitoring Management	1	0	5	6
Plan of Action and Milestones	0	3	0	3
Contractor Systems	0	1	0	1
Incident Response and Reporting	0	0	1	1
Security Training	0	0	1	1
Remote Access Management	0	0	0	0

Note: Totals do not equal the number of reports and testimonies identified because one report or testimony may cover several FISMA reporting metrics.

Frequently Cited Cybersecurity Weaknesses

The reports and testimony issued during the reporting period most frequently cited weaknesses in the FISMA reporting metrics of risk management, identity and access management, and contingency planning. See Appendix B for a matrix of reports listed by their specific cybersecurity weaknesses and Appendix C for a list of reports and testimony summarized in this report.

Risk Management

Risk Management is the process of managing threats to organizational operations, organizational assets, other organizations, individuals, and the United States, that result from operating an information system. Risk management includes:

- performance of a risk assessment,
- implementation of a risk mitigation strategy, and
- employment of techniques and procedures for the continuous monitoring of the information system's security.

The DoD audit community and GAO reported risk management weaknesses in 17 reports, and made 36 recommendations. Examples of those weaknesses are contained in the following two reports.

DoD Needed to Reinitiate Migration to Internet Protocol Version 6

DoDIG Report DODIG-2015-044, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6," December 1, 2014, identified that DoD had not completed the Federal and DoD requirements to effectively migrate the DoD enterprise network to Internet Protocol Version 6 (IPv6). The Federal and DoD requirements were not completed because the DoD Chief Information Officer (CIO) and U.S. Cyber Command had not made IPv6 a priority. Further, the DoD CIO did not have a current plan of action and milestones to advance DoD IPv6 migration efforts.

According to the report, the continued use of IPv4 will delay the potential benefits of IPv6, such as improved communication, warfighter mobility, situational awareness, and quality of service. Cyber and IPv6 subject matter experts agreed that IPv4 cannot support future networking and combat system demands. Further, the delay in migration could increase DoD's costs and its vulnerability to adversaries.

The DoD OIG recommended that the DoD CIO:

- establish a DoD-wide IPv6 transition office and working group to advance DoD's transition to IPv6;
- establish a process to integrate component testing results and lessons learned into DoD IPv6 migration efforts; and
- develop new DoD IPv6 transition milestones, roles and responsibilities of each DoD office involved with migration, and enforcement mechanisms to ensure successful migrations to IPv6, and update the DoD IPv6 Transition Plan to reflect the changes.

Although the DoD CIO disagreed with establishing a DoD-wide IPv6 transition office, the DoD CIO had initiated a steering group, which DoD OIG determined fully addressed the intent of the recommendation. For the additional two recommendations, the DoD CIO agreed to continue to work with the various test centers to assess IPv6 threats to develop appropriate countermeasures. In addition, the DoD CIO agreed to draft and coordinate a memorandum with transition milestones, roles, responsibilities, and enforcement mechanisms for each DoD office involved in the IPv6 implementation.

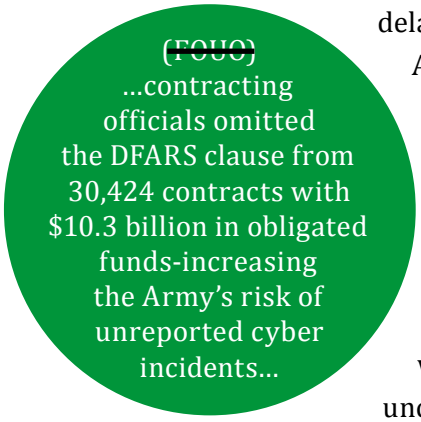
Army Contracting Office Had Not Included Defense Federal Acquisition Regulation Supplement Clause for Cyber Reporting in Contracts

~~(FOUO)~~ Army Audit Agency (AAA) Report No. A-2015-0034-IET, "Audit of Cyber Interactions with Defense Industry Partners," February 13, 2015, identified that Army organizations historically relied on contractors to voluntarily share identified cyber threat information using the Defense Industrial Base Voluntary Cyber Security/Information Assurance Program (DIB CS/IA), to "harden" their respective unclassified networks. The DIB CS/IA began in 2007 with 16 companies as a collaborative environment in which information that affects the Global Information Grid and participating contractor networks could be shared. In 2012, DoD expanded the program to include cleared defense contractors, and by August 2014, more than 100 defense industry partners and subsidiaries had entered into the voluntary program.

~~(FOUO)~~ The FY 2013 National Defense Authorization Act addressed concern from Congress for DoD to ensure it maintained full visibility and control of its supply chain to mitigate supply chain exploitation. It also addressed DoD's need for the authority and capability to mitigate supply chain risks to its computerized systems that fall outside the scope of National Security systems. The FY 2013 National

(~~FOUO~~) Defense Authorization Act section 941 required the Secretary of Defense to establish procedures that required defense contractors to report to DoD when a contractor's network was successfully penetrated. In November 2013, the Office of Defense Procurement and Acquisition Policy released Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which requires contractors with controlled technical information[2] to report all cyber incidents within 72 hours of discovery.

(~~FOUO~~) However, the report states some Army contract officials delayed adding the DFARS clause to contracts awarded until September 2014, because the Deputy Assistant Secretary of Army, Procurement (DASA (P)) delayed issuing Policy Alert 14-75[3] until September 2014. According to the report, the Policy Alert instructs contracting officers to include the DFARS clause in future contracts and solicitations. In the absence of guidance, contracting officials omitted the DFARS clause from 30,424 contracts with $10.3 billion in obligated funds-increasing the Army's risk of unreported cyber incidents associated with controlled technical data on a contractor's unclassified network.



(~~FOUO~~) AAA recommended the DASA (P) develop a risk-based approach to review the 30,424 contracts that were awarded without the DFARS clause and update the highest-risk contracts to add the clause. According to the report, DASA (P), Policy and Enterprise Business System Directorates stated they would use an established risk-based approach to identify the high-risk solicitations and contracts issued after November 2013, and require the command to insert the DFARS clause in those solicitations and contracts.

Identity and Access Management

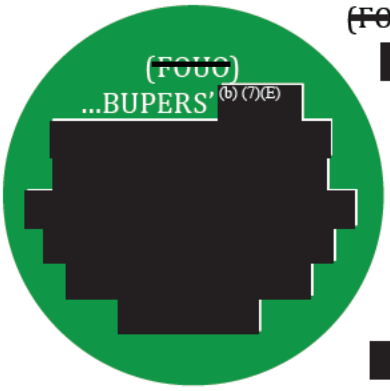
Identity and access management includes the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources. The DoD audit community and GAO reported weaknesses related to identity and access management in 11 reports, and made 26 recommendations. Examples of those weaknesses are contained in the following two reports.

[2] Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

[3] Policy Alert 14-75, "Safeguarding Unclassified Controlled Technical Information," September 9, 2014.

Navy Bureau of Personnel Had Not Implemented Effective Management Controls for Navy Corporate Data

~~(FOUO)~~ Naval Audit Service (NAS) Report No. N2015-0026, "Management Controls of Navy Corporate Data," July 16, 2015, identified weaknesses in the process (b) (7)(E) to the Navy Bureau of Personnel (BUPERS) (b) (7)(E) System. The (b) (7)(E) System is comprised of (b) (7)(E) IT systems ((b) (7)(E) classified) containing personnel data with (b) (7)(E). In accordance with Navy guidance, individuals are required[4] to complete a System Authorization Access Request-Navy (SAAR-N) form[5] to gain access to Navy IT systems. The report states that BUPERS had not (b) (7)(E). Furthermore, SAAR-N forms provided by BUPERS personnel to the audit team were incomplete.



~~(FOUO)~~ NAS determined that BUPERS' (b) (7)(E). Further, BUPERS did not follow (b) (7)(E) and there was no standard written process for how SAAR-N forms should be completed and approved. (b) (7)(E). According to the report, this made BUPERS vulnerable (b) (7)(E).

~~(FOUO)~~ NAS recommended that the Deputy, Chief of Naval Personnel develop and implement controls to ensure (b) (7)(E) Systems as required by DoD Instruction 8500.2 and Secretary of the Navy Manual 5239.1. In response to the recommendations, the Deputy, Chief of Naval Personnel stated they would draft a BUPERS Instruction to provide specific guidelines for the correct completion of the SAAR-N.

[4] All Commands 170/11, "Navy Telecommunications Directive, System Authorization Access Request-Navy (SAAR-N)," October 2011.

[5] The SAAR-N form identifies the following information: having a need-to-know, completion of the annual information assurance training, and at least the minimum required security clearance. This information is used to determine the individual's access.

Air Force Automated Civil Engineering System Personnel Had Not Effectively Implemented Application-Level General Controls

Air Force Audit Agency (AFAA) Report No. F2015-0003-O10000, "Automated Civil Engineering System-Real Property Application Controls," March 9, 2015, identified that Automated Civil Engineer System-Real Property (ACES-RP) personnel had not effectively implemented security management, access controls, configuration management, segregation of duties, and contingency planning in accordance with National Institute of Standards and Technology (NIST) guidance. Specifically, for access controls, ACES-RP personnel had not:

- used or maintained user access forms, or
- reviewed account access periodically to ensure continued appropriateness as required by NIST SP 800-53.[6]

According to the report, the controls were not effectively implemented because ACES-RP program management personnel had not applied the NIST Risk Management Framework. The report concluded that ACES-RP application control discrepancies cast doubt on the reliability of operational mission data used to track all Air Force real property.

AFAA recommended that the Deputy Chief of Staff for Logistics, Installations, and Mission Support (AF/A4) direct ACES-RP program personnel to develop a complete security management, configuration management and contingency plan; require and maintain user access forms; perform account reviews; and develop a segregation of duties matrix. According to the report, AF/A4 provided the AFAA with their corrective action plans, which addressed the recommendations.

Contingency Planning

Contingency planning is the process of preparing for emergency response, backup operations, and post-disaster recovery of an information system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation. The DoD audit community and GAO reported weaknesses related to contingency planning in seven reports and one testimony, and made 15 recommendations. Examples of those weaknesses are contained in the following two reports.

[6] NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

DoD Had Not Aligned Guidance for Preparing for and Responding to Domestic Cyber Incidents

GAO testimony GAO-15-686T, "Civil Support: DoD is Taking Action to Strengthen Support of Civil Authorities," June 10, 2015, contains testimony presented by the GAO Director of Defense Capabilities and Management to the Subcommittee on Emergency Preparedness, Response, and Communications, Committee on Homeland Security. The Director's testimony was based on five GAO reports issued from March 2010 through December 2014 that examined DoD's Defense Support of Civilian Authorities mission.[7] The Director testified on DoD's progress to implement recommendations GAO made in previous reports to strengthen (1) DoD's strategy, plans, and guidance documents; (2) interagency coordination; and, (3) capabilities to support civil authorities.

The Director specifically cited an October 2012 report,[8] where GAO identified that DoD had not updated its Defense Support of Civilian Authorities guidance to ensure that it was consistent with national plans and preparations for domestic cyber incidents. As a result, GAO recommended DoD align guidance on preparing for and responding to domestic incidents with national-level guidance to include roles and responsibilities. As of June 2015, DoD had not taken action that met the intent of the recommendation.

Air Force Commanders Resource Integration System Personnel Had Not Fully Implemented a Contingency Plan

AFAA Report No. F2015-0006-O10000, "Commanders Resource Integration System Application Controls," March 10, 2015, identified that the Commanders Resource Integration System (CRIS) personnel did not effectively implement application-level general controls that included security management, access controls, and contingency planning in accordance with NIST guidance. Specifically, the report

[7] Defense support of civil authorities is support provided by federal military forces, DoD civilians, DoD contract personnel, DoD component assets, and, in certain circumstances, National Guard forces in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

[8] GAO Report GAO-13-128, "DoD Needs to Address Gaps in Homeland Defense and Civil Support Guidance," October 24, 2012.

...program management office personnel had not properly tested the system contingency plan.

stated that a 2013 contingency test did not include: system recovery on an alternate platform from backup media, coordination among recovery teams, internal and external connectivity, system performance using alternate equipment, and restoration of normal operations. Further, program management office personnel had not properly tested the system contingency plan.

AFAA determined that CRIS personnel had not:

- implemented NIST Risk Management Framework.[9]
- categorized the system risk, selected and implemented the appropriate controls, or assessed those application controls as required by NIST and FISMA.
- complied with the May 31, 2013 SAF/FM memorandum[10] directing all Air Force information technology system program offices and functional managers to comply with existing GAO FISCAM[11]-identified requirements and other applicable financial systems standards.

The report also states that CRIS personnel followed the DoD 8500-series policies, which did not reflect current Federal regulations for application-level general and interface controls.

According to the report, without a proper CRIS contingency plan, system outages could result in critical logistics mission failure. The AFAA recommended that SAF/FM direct CRIS program and functional personnel to follow the Federal NIST system control standards detailed in updated DoD Instruction 8510.01, published in March 2014 and the May 31, 2013, SAF/FM memorandum. In addition, AFAA recommended that SAF/FM develop a complete security management and contingency plan; require and maintain user access forms and perform account reviews. According to the report, SAF/FM provided the AFAA with their corrective action plans, which addressed the recommendations.

[9] NIST Special Publication 800-37, "Guide for Applying Risk Management Framework (RMF) to Federal Information Systems," February 2010.

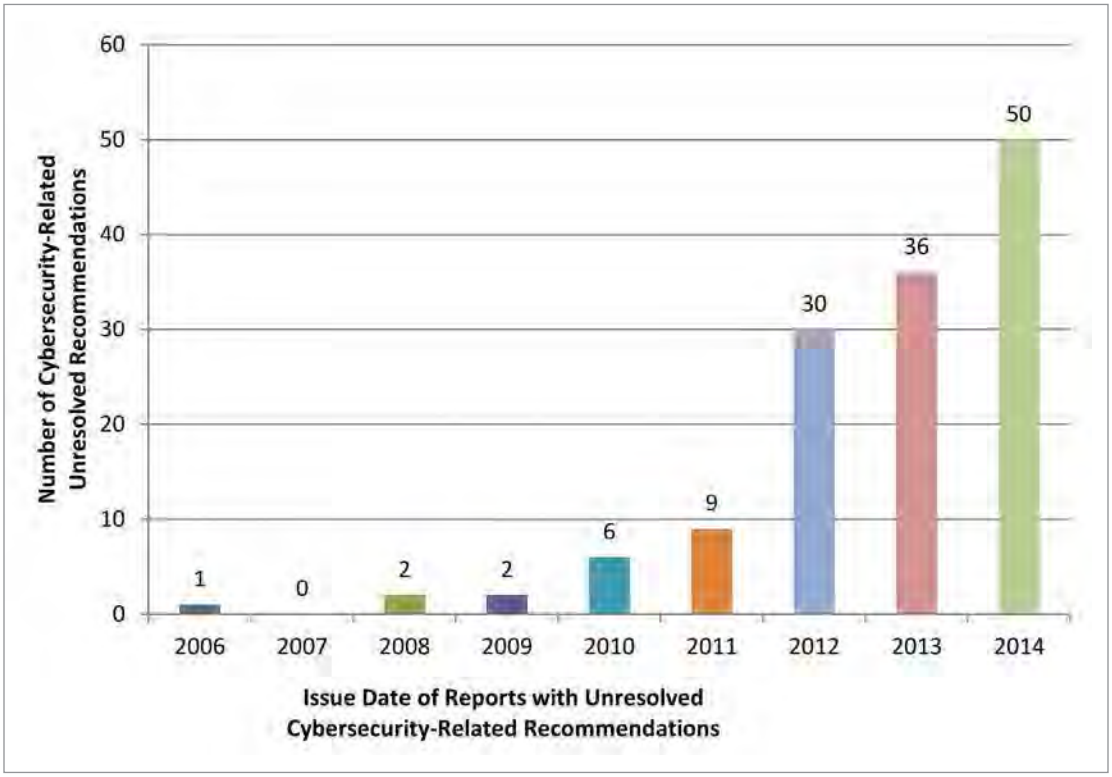
[10] SAF/FM Memorandum, "Information Technology-Financial Controls and Accounting Conformance Guidance," May 31, 2013.

[11] GAO-09-232G, "Federal Information System Controls Audit Manual (FISCAM)," February 2009.

DoD's Progress to Implement Recommendations Reported in Previously Issued Cybersecurity Summary Reports

As of August 1, 2014, audit reports included in the previously issued cybersecurity summary reports contained 229 unresolved cybersecurity-related recommendations. From August 1, 2014, through July 31, 2015, DoD management resolved 93 of those recommendations, leaving 136 unresolved cybersecurity-related recommendations that required management action. See the figure for the issue date of reports containing the remaining 136 unresolved cybersecurity-related recommendations. See Appendix D for a list of the reports containing unresolved recommendations.

Figure. Issue Date of Reports Containing Unresolved Recommendations Related to Cybersecurity Weaknesses



Cybersecurity Weaknesses Identified in Unresolved Recommendations

The most common cybersecurity weaknesses identified in the 136 unresolved recommendations are related to the FY 2015 FISMA metrics of risk management, identity and access management, and configuration management. Table 2 identifies the cybersecurity weaknesses as they relate to the unresolved recommendations.

Table 2. Cybersecurity Weaknesses Identified in Unresolved Recommendations

FISMA Reporting Metrics	GAO	DoD OIG	Military Departments	Total
Risk Management	2	25	36	63
Identity and Access Management	0	22	27	49
Configuration Management	2	11	12	25
Plan of Action & Milestones (POA&M)	1	17	2	20
Contingency Planning	4	0	15	19
Security Training	0	3	9	12
Continuous Monitoring Management	0	7	2	9
Incident Response and Reporting	1	4	4	9
Contractor Systems	0	1	2	3
Remote Access Management	0	0	1	1

Note: Totals do not equal the number of reports and testimonies identified because one report or testimony may cover several metrics.

Summary

The DoD audit community and GAO issued 20 unclassified reports and one testimony from August 1, 2014, through July 31, 2015, that identified cybersecurity weaknesses related to the FY 2015 FISMA Inspector General reporting metrics. Within the reports and testimony, risk management, identity and access management, and contingency planning were the most frequently cited cybersecurity weaknesses. Furthermore, the DoD audit community and GAO provided 49 recommendations to correct the identified cybersecurity weaknesses, and DoD continues to make progress in addressing those recommendations.

Appendix A

Scope and Methodology

We conducted this summary work from May 2015 through September 2015. We followed generally accepted government auditing standards, except for the standards of planning and evidence because the report summarizes previously released reports. This summary report supports the DoD OIG response to the requirements of Public Law 107-347, section 3545, Title III, "Federal Information Security Management Act (FISMA) of 2002," December 17, 2002.

Also, this report summarizes the DoD cybersecurity weaknesses identified in 20 unclassified reports and one testimony that GAO and the DoD audit community issued from August 1, 2014, through July 31, 2015. To prepare this summary, we reviewed the websites of GAO and each DoD Component audit organization and requested reports discussing cybersecurity weakness reports. We did not review the supporting documentation for any of the reports. This summary report does not contain recommendations because the summarized reports contained recommendations related to the cybersecurity weaknesses identified.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, DoD OIG issued five reports summarizing cybersecurity weaknesses identified in 179 audit reports and testimonies issued by the DoD audit community and the GAO. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm. The following reports are For Official Use Only (FOUO) and can be obtained through the Freedom of Information Act Requestor Service website at https://www.dodig.mil/foia/submitfoia.html.

DoD IG

Report No. DODIG-2014-126, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2013, Through July 31, 2014," September 26, 2014 (Report is FOUO)

Report No. DODIG-2013-141, "DoD Information Assurance Weakness as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013," September 30, 2013 (Report is FOUO)

Report No. DODIG-2012-145, "DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2011, Through July 31, 2012," September 27, 2012 (Report is FOUO)

Report No. D-2011-114, "Summary of Information Assurance Weaknesses Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011," September 30, 2011

Report No. D-2010-090, "Summary of Information Assurance Weaknesses Identified in Audit Reports Issued From August 1, 2009, Through July 31, 2010," September 30, 2010 (Report is FOUO)

Appendix B

Matrix of Cybersecurity Weaknesses Reported From August 1, 2014, Through July 31, 2015

Agency Report No.	FISMA Reporting Metrics									
	Configuration Management	Contingency Planning	Continuous Monitoring Management	Contractor Systems	Identity and Access Management	Incident Response and Reporting	Plan of Action and Milestones	Remote Access Management	Risk Management	Security Training
Government Accountability Office										
GAO-15-749									X	
GAO-15-544			X						X	
GAO-15-686T		X								
DoD Inspector General										
DODIG-2015-102					X					
DODIG-2015-045				X			X		X	
DODIG-2015-044	X						X		X	
DODIG-2015-008	X						X			
Army Audit Agency										
A-2015-0034-IET						X			X	
Naval Audit Service										
N2015-0027									X	
N2015-0026					X				X	X
N2015-0017									X	
N2014-0047					X					

Matrix of Cybersecurity Weaknesses Reported From August 1, 2014, Through July 31, 2015 (cont'd)

Agency Report No.	FISMA Reporting Metrics									
	Configuration Management	Contingency Planning	Continuous Monitoring Management	Contractor Systems	Identity and Access Management	Incident Response and Reporting	Plan of Action and Milestones	Remote Access Management	Risk Management	Security Training
Air Force Audit Agency										
F2015-0010-O10000	X	X	X		X				X	
F2015-0009-O10000	X	X	X		X				X	
F2015-0008-O10000	X	X	X		X				X	
F2015-0007-O10000									X	
F2015-0006-O10000		X			X				X	
F2015-0005-O10000		X	X		X				X	
F2015-0004-O10000					X				X	
F2015-0003-O10000	X	X			X				X	
F2015-0001-O10000	X	X	X		X				X	
Total	**7**	**8**	**6**	**1**	**11**	**1**	**3**	**0**	**17**	**1**

Note: Totals do not equal the number of reports and testimonies identified because one report or testimony may cover several FY 2015 reporting metrics.

Appendix C

Audit Reports Issued From August 1, 2014, Through July 31, 2015

Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted AAA reports can be accessed from .mil and gao.gov domains at https://www.aaa.army.mil/. NAS and AFAA reports are unavailable over the Internet. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

Report No. GAO-15-749, "Defense Infrastructure: Improvements in DoD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning," July 2015

Report No. GAO-15-544, "Insider Threats: DoD Should Strengthen Management and Guidance to Protect Classified Information and Systems," June 2015

DoD IG

Report No. DODIG-2015-102, "Additional Actions Needed to Effectively Reconcile Navy's Fund Balance With Treasury Account," April 3, 2015

Report No. DODIG-2015-045, "DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process," December 4, 2014

Report No. DODIG-2015-044, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6," December 1, 2014 (Report is FOUO)

Report No. DODIG-2015-008, "Followup Audit: Enterprise Blood Management System Not Ready for Full Deployment," October 23, 2014

Army Audit Agency

Report No. A-2015-0034-IET, "Audit of Cyber Interactions with Defense Industry Partners," February 13, 2015 (Report is FOUO)

Naval Audit Service

Report No. N2015-0027, "Followup on Naval Audit Service Report N2012-0009, 'Personally Identifiable Information and Department of the Navy Data on Unencrypted Computer Hard Drives Released from Department of the Navy Control,'" July 23, 2015 (Report is FOUO)

Report No. N2015-0026, "Management Controls of Navy Corporate Data," July 16, 2015 (Report is FOUO)

Report No. N2015-0017, "Technology Readiness Assessments at Naval Sea Systems Command and Affiliated Program Executive Offices," April 2, 2015 (Report is FOUO)

Report No. N2014-0047, "Marine Corps Military Standard Requisitioning and Issue Procedures Internal Controls," September 30, 2014 (Report is FOUO)

Air Force Audit Agency

Report No. F2015-0009-O10000, "Stock Control System Application Controls," April 2, 2015

Report No. F2015-0010-O10000, "Depot Maintenance and Production System – Time and Attendance Application Controls," April 2, 2015

Report No. F2015-0004-O10000, "Automated Contract Preparation System Application Controls," March 10, 2015

Report No. F2015-0005-O10000, "Contract Writing System Application Controls," March 10, 2015

Report No. F2015-0006-O10000, "Commanders Resource Integration System Application Controls," March 10, 2015

Report No. F2015-0007-O10000, "Standard Procurement System Application Controls," March 10, 2015

Report No. F2015-0008-O10000, "Military Personnel Data System Application Controls," March 10, 2015

Report No. F2015-0003-O10000, "Automated Civil Engineering System-Real Property Application Controls," March 9, 2015

Report No. F2015-0001-O10000, "Cargo Movement Operations System Application Controls," December 15, 2014

GAO Testimony

Report No. GAO-15-686T, "Civil Support: DoD is Taking Action to Strengthen Support of Civil Authorities," June 10, 2015

Appendix D

Audit Reports From Prior Cybersecurity Summary Reports With Unresolved Recommendations

As of August 1, 2014, previously identified audit reports contained 229 unresolved cybersecurity-related recommendations. During the reporting period of August 1, 2014, through July 31, 2015, management resolved 93 recommendations, leaving 136 unresolved cybersecurity-related recommendations. These 136 unresolved recommendations are contained in the 51 audit reports listed below. The list of reports with unresolved recommendations were compiled based on information GAO and the DoD Audit community provided in August 2015 and may be incomplete because of the extent of information maintained in their respective follow-up systems.

Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted AAA reports can be accessed from .mil and gao.gov domains at https://www.aaa.army.mil/. NAS and AFAA reports are unavailable over the Internet. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

Report No. GAO-14-404SU, "Defense Cybersecurity: DoD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight," April 2014 (Report is FOUO)

Report No. GAO-14-182, "Defense Logistics: Actions Needed to Improve Department-Wide Management of Conventional Ammunition Inventory," March 2014

Report No. GAO-12-992, "VA and DoD Health Care: Department-Level Actions Needed to Assess Collaboration Performance, Address Barriers, and Identify Opportunities," September 2012

Report No. GAO-12-669, "VA/DoD Federal Health Care Center: Costly Information Technology Delays Continue and Evaluation Plan Lacking," June 2012

Report No. GAO-11-621, "Intelligence, Surveillance, and Reconnaissance: DoD Needs a Strategic, Risk-Based Approach to Enhance Its Maritime Domain Awareness," June 2011

Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011

DoD IG

Report No. DODIG-2014-066, "Logistic Modernization Program System Not Configured to Support Statement of Budgetary Resources," May 5, 2014

Report No. DODIG-2014-037, "Systemic Weaknesses Leave Civil Works Infrastructure Vulnerable to Physical and Cyber Attacks," February 10, 2014 (Report is FOUO)

Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013

Report No. DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," September 16, 2013 (Report is FOUO)

Report No. DODIG-2013-130, "Army Needs to Improve Controls and Audit Trails for the General Fund Enterprise Business System Acquire-to-Retire Business Process," September 13, 2013

Report No. DODIG-2013-109, "Improved Security Needed to Protect Infrastructure and Systems in the Great Lakes and Ohio River Division," July 29, 2013 (Report is FOUO)

Report No. DODIG-2013-072, "Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System," April 24, 2013 (Report is FOUO)

Report No. DODIG-2013-036, "Improvements are Needed to Strengthen Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division," January 14, 2013 (Report is FOUO)

Report No. DODIG-2012-122, "DoD Should Procure Compliant Physical Access Control Systems to Reduce the Risk of Unauthorized Access," August 29, 2012 (Report is FOUO)

Report No. D-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012 (Report is FOUO)

Report No. D-2012-050, "Improvements Needed With Host-Based Intrusion Detection Systems," February 3, 2012 (Report is FOUO)

Report No. D-2011-096, "Improvements Are Needed to the DoD Information Assurance Vulnerability Management Program," August 12, 2011 (Report is FOUO)

Report No. D-2011-089, "Reducing Vulnerabilities at the Defense Information Systems Agency Defense Enterprise Computing Centers," July 22, 2011 (Report is FOUO)

Army Audit Agency

Report No. A-2014-0034-FMT, "Data Spillage," January 7, 2014 (Report is FOUO)

Report No. A-2013-0130-FMR, "Miscellaneous Pay Process General Fund Enterprise Business System," July 31, 2013

Naval Audit Service

Report No. N2014-0029, "Internal Controls for Overtime Benefits Received at Norfolk Naval Shipyard and Portsmouth Naval Shipyard," July 1, 2014 (Report is FOUO)

Report No. N2014-0022, "Fleet Gapped Critical Billets," May 20, 2014 (Report is FOUO)

Report No. N2014-0021, "Cyberspace/Information Technology Skill Sets for Active Duty Military Personnel at Selected Navy Commands," May 19, 2014 (Report is FOUO)

Report No. N2013-0050, "Long-Term Temporary Duty Orders for Marine Corps Reserves Performing Duty within the Continental United States and Hawaii," September 30, 2013 (Report is FOUO)

Report No. N2012-0070, "Navy Compliance with Department of Defense Information Assurance Certification and Accreditation Process," September 28, 2012 (Report is FOUO)

Report No. N2012-0010, "Defense Travel System-Marine Corps," December 21, 2011 (Report is FOUO)

Report No. N2011-0046, "Followup of Management of Personally Identifiable Information at Marine Corps Recruiting Command," July 29, 2011 (Report is FOUO)

Report No. N2008-0023, "Information Security within the Marine Corps," February 20, 2008

Air Force Audit Agency

Report No. F2014-0005-O10000, "Standard Procurement System General and Selected Application Controls," December 3, 2013

Report No. F2014-0003-O10000, "Memorandum Report of Audit F2014-0003-O10000, Integrated Logistics System-Supply Application Controls," November 1, 2013

Report No. F2014-0004-O10000, "Memorandum Report of Audit F2014-0004-O10000, Automated Contract Preparation System General and Application-Level General Controls," November 1, 2013

Report No. F2013-00016-O40000, "Memorandum Report of Audit F2013-0016-O40000, Reserve Travel System – Phase 1, General and Selected Application Controls," September 5, 2013

Report No. F2013-0003-L20000, "Serialized Parts Configuration Management," April 1, 2013

Report No. F2013-0011-O10000, "Memorandum Report of Audit F2013-0011-O10000, Integrated Missile Database System Application Controls," January 15, 2013

Report No. F2013-0009-O10000, "Memorandum Report of Audit F2013-0009-O10000, Reliability, Availability, Maintainability Support System for Electronic Combat Pods-Application Controls," January 3, 2013

Report No. F2013-0007-O10000, "Memorandum Report of Audit F2013-0007-O10000, Financial Inventory Accounting and Billing System Application Controls," November 20, 2012

Report No. F2013-0005-O10000, "Enterprise Information Protection Capability," October 26, 2012

Report No. F2013-0003-O10000, "Memorandum Report of Audit F2013-0003-O10000, Reliability and Maintainability Information System Application Control," October 22, 2012

Report No. F2012-0009-FB2000, "Memorandum Report of Audit F2012-0009-FB2000, Automated Funds Management General Controls," June 26, 2012

Report No. F2012-0006-FB2000, "Memorandum Report of Audit F2012-0006-FB2000, Positive Inventory Control Fusion - Application Controls," April 12, 2012

Report No. F2012-0005-FB2000, "Memorandum Report of Audit F2012-0005-FB2000, Automated Funds Management Application Controls," April 4, 2012

Report No. F2012-0003-FB4000, "System Vulnerability Detection and Mitigation," February 16, 2012

Report No. F2012-0003-FB2000, "Defense Enterprise Accounting and Management System Selected System Controls," January 17, 2012

Report No. F2012-0002-FB4000, "Air National Guard Information Systems Security," January 11, 2012

Report No. F2011-0004-FB4000, "Computer Network Incident Response and Reporting," April 20, 2011

Report No. F2010-0009-FB2000, "Implementation of Chief Financial Officer Compliance Tracking for Financial Systems," July 28, 2010

Report No. F2010-0005-FB4000, "Publicly Accessible Air Force Web Sites," May 14, 2010

Report No. F2010-0003-FB4000, "Contractor Circuit Security," January 13, 2010

Report No. F2009-0004-FB2000, "Defense Enterprise Accounting and Management System Controls," February 20, 2009

Report No. F2006-0006-FB2000, "Controls for the Wholesale and Retail Receiving and Shipping System," May 19, 2006

Glossary

Configuration Management: the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

Contingency Planning: the process of preparing for emergency response, backup operations, and post-disaster recovery of an information system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Continuous Monitoring: the process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: (1) the development of a strategy to regularly evaluate selected information assurance controls/metrics; (2) recording and evaluating information assurance-relevant events and the effectiveness of the enterprise in dealing with those events; (3) recording changes information assurance controls, or changes that affect information assurance risks; and (4) publishing the current security status to enable information sharing decisions involving the enterprise.

Contractor Systems: agency systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in a cloud external to the agency.

Identity and Access Management: the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources.

Incident Response and Reporting: the mitigation of violations of security policies and recommended practices; also referred to as incident handling.

Plan of Action and Milestones: a tool that identifies tasks that need to be accomplished. A plan of action and milestones details resources required to accomplish the plan elements, task milestones, and milestone completion dates. The purpose of a plan of action and milestones is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Remote Access Management: access to organizational information system by a user (or a process acting on behalf of a user) communicating through an external network, such as the Internet.

Risk Management: the process of managing threats to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organization, and the Nation, resulting from information system operations, and includes: (1) the performance of a risk assessment; (2) the implementation of a risk mitigation strategy, (3) employment of techniques and procedures for the continuous monitoring of the information system's security state; (4) documenting of the overall risk management program.

Security Training: formal activities, products, and services intended to create or enhance the security knowledge or skills of persons or raise their level of performance, motivation, or operations.

Acronyms and Abbreviations

AAA	Army Audit Agency
ACES-RP	Automated Civil Engineer System-Real Property
AFAA	Air Force Audit Agency
BUPERS	Bureau of Personnel
CIO	Chief Information Officer
DFARS	Defense Federal Acquisition Regulation Supplement
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IT	Information Technology
NAS	Naval Audit Service
NIST	National Institute of Standards and Technology
SAAR-N	System Authorization Access Request-Navy


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL
4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098